UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

Federal Trade Commission **Plaintiff,** **v.** **Innovative Marketing, Inc., *et al.*** **Defendants,** **AND** **Maurice D'Souza** **Relief Defendant.**	**CIVIL NO.**

MEMORANDUM OF LAW IN SUPPORT OF
PLAINTIFF'S *EX PARTE* MOTION FOR TRO AND ORDER TO SHOW CAUSE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

STATUTES

I. SUMMARY

Plaintiff Federal Trade Commission ("FTC" or "Commission") seeks an *ex parte* temporary restraining order ("TRO") to bring an immediate halt to an unlawful, Internet-based, deceptive advertising scheme that has flooded the Internet with hundreds of millions of deceptive ads, ensnared more than one million consumer victims, and caused more than $100 million in consumer injury.

Defendants masquerade as Internet advertising agencies seeking to place ads on behalf of legitimate companies. Although the ads placed by Defendants appear legitimate, they are in fact trojan horses that contain hidden code capable of involuntarily redirecting consumers away from the websites they are viewing and transporting them to one of the Defendants' websites. After hijacking consumers, Defendants display a convincing but utterly bogus "system scan" that purports to scan consumers' computers for harmful and illegal files. Invariably, these bogus scans falsely report that consumers' computers are filled with viruses, spyware or pornography.

To cure the security problems "detected" by the bogus scanner, Defendants instruct consumers to purchase their computer security software, which goes by a variety of names such as WinFixer, WinAntiVirus, DriveCleaner, ErrorProtector, SystemDoctor, XP AntiVirus, and AdvancedCleaner. These security products – known in Internet parlance as "scareware" due to the deceitful manner in which they are marketed – are sold at a cost of $39.95 or more.

Because Defendants operate a business permeated by fraud that exists solely to swindle unsuspecting consumers, the Commission seeks an *ex parte* temporary restraining order to freeze assets and to preserve evidence. Defendants' continued use of blatantly deceptive advertising, extensive efforts to hide from disgruntled consumers and law enforcement, duplicity in dealing with ad networks and websites, and history of illegal conduct, demonstrate their propensity to violate the law and to disregard any order to refrain from dissipating or concealing assets or destroying documents if given advance notice of this lawsuit. Accordingly, immediate, *ex parte* relief is critical to bringing a halt to Defendants' deception, and to protect Defendants' assets for possible consumer redress pending final

resolution of this matter.

II. THE PARTIES

A. Plaintiff

Plaintiff, FTC, is an independent agency of the United States government created by the FTC Act, 15 U.S.C. §§ 41 - 58. The FTC is charged with, among other things, enforcement of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act, and to secure such equitable relief as may be appropriate in each case, including restitution and disgorgement. 15 U.S.C. § 53(b).

B. Defendants and the Relief Defendant

Corporate defendant Innovative Marketing, Inc. ("IMI") is a corporation incorporated pursuant to the laws of Belize and headquartered in the Ukraine. Drexler Decl., Ex. 20, ¶¶ 34, 37. IMI deceptively markets and sells its products to consumers around the world, including consumers in Maryland. Drexler Decl., Ex. 20, ¶ 26; Layton Decl., Ex. 1.

Corporate defendant ByteHosting Internet Services, LLC ("ByteHosting") is an Ohio limited liability company located in Cincinnati, Ohio that is owned by James Reno. Drexler Decl., Ex. 20, ¶ 56, 82. Defendant ByteHosting operates as a common enterprise with defendant Innovative Marketing (collectively, the "IMI Enterprise"), and does business in this district. Layton Decl., Ex. 1.

Defendant Daniel Sundin has lived in the United States but now resides in London, England. Drexler Decl., Ex. 20, ¶¶ 34, 35. Sundin has served as the Chief Operating Officer, and currently serves as the Chief Technology Officer, of IMI. Id. at ¶ 34.

Defendant Sam Jain is a California resident. Drexler Decl., Ex. 20, ¶ 101. Jain is the Chief Executive Officer of IMI. Drexler Decl., Ex. 20, ¶ 98.

Defendant Marc D'Souza is a resident of Ontario, Canada. Drexler Decl., Ex. 20, ¶ 121. D'Souza was a senior executive with IMI until December 2006, when he split from the company. Id. at ¶¶ 122,

124. Until his departure, D'Souza functioned as the Chief Financial Officer and Chief Marketing Officer of IMI. Id. at ¶ 124.

Defendant Kristy Ross is a United States citizen residing in Maryland. Drexler Decl., Ex. 20, ¶ 114. Ross is the Vice President of Business Development for IMI and has recently assumed some of Defendant Sundin's responsibilities as Chief Operating Officer of IMI. Id. at ¶¶ 107 - 08.

Defendant James Reno is a resident of Ohio, and is the owner of ByteHosting. Drexler Decl., Ex. 20, ¶¶ 65, 67. Reno oversees several business critical functions on behalf of the IMI Enterprise, including key contracts with vendors and the IMI Enterprise's call center. Id. at ¶¶ 71, 78, 82.

Relief defendant Maurice D'Souza, father of defendant Marc D'Souza, is a resident of Ontario, Canada. Drexler Decl., Ex. 20, ¶¶ 125, 129. Maurice D'Souza holds millions of dollars of proceeds from the IMI Enterprise in bank accounts he controls. Id. at ¶ 131.

III. THE DEFENDANTS' BUSINESS PRACTICES

Defendants trick consumers into purchasing their security software by displaying to consumers fake "system scans" that purport to scan consumers' computers and invariably detect a host of urgent security and/or privacy problems, such as viruses, spyware or "illegal" pornography. In many cases, these false representations are repeated in a software-based scan that Defendants display after their products are downloaded to consumers' computers. At the completion of these bogus scans, Defendants aggressively market their security software, at a cost of $39.95 or more, to consumers as a cure for the ills purportedly detected by the scanners. Unaware of Defendants' trickery, more than one million consumers have been duped into purchasing Defendants' products. Drexler Decl., Ex. 20, ¶ 58.

A. Consumer Complaints

The FTC has received more than 1,000 consumer complaints about the Defendants' products and advertising. Drexler Decl., Ex. 20, ¶ 26. Consumers complain of receiving unsolicited pop-up windows

while using their computers.[1] These windows display an elaborate scan of consumers' computers that purports to detect viruses, trojans or pornography.[2] Consumers report that at the completion of the scans they are urged to purchase one of Defendants' security products in order to remedy the critical threats detected by the scanner.[3] Consumers report seeing a number of Defendants' products marketed in this fashion, including "AntiVirus 2008," "SystemDoctor," "DriveCleaner," "AdvancedCleaner," "XP Antivirus 2008," "WinAntiVirus," and "WinAntiVirus PRO."[4]

Consumer Cynthia Randall's story is typical. In March 2008, Randall was surfing the Internet when she was redirected to a website she did not enter into her browser. Randall Decl., Ex. 8, ¶ 2. This webpage commenced a scan of her computer and purported to detect several viruses as well as out of date anti-virus software. Id. at ¶ 3. The webpage then urged Randall to purchase Defendants' XP Antivirus 2008 program in order to remove the infection. Id. at ¶ 4. Randall recognized that the color scheme and appearance of the scanner matched Microsoft Windows, and assumed that the scan was conducted by a Microsoft product. Id. at ¶ 5. To protect her computer, Randall proceeded to purchase XP Antivirus 2008 for $49.95 using her credit card. Id. at ¶ 6. When Randall attempted to download

---

[1]Church Decl., Ex. 2, ¶¶ 2-3; Davis Decl., Ex. 3, ¶ 2-3; Hurd Decl., Ex. 4, ¶ 3; Layton Decl., Ex 1, ¶¶ 6, 10; Marcynzsyn Decl., Ex. 5, ¶¶ 3 - 4; Mullen Decl., Ex. 6, ¶¶ 2-4; Pritchett Decl., Ex. 7, ¶¶ 2-3; Randall Decl., Ex. 8, ¶¶ 2-4; Renteria Decl., Ex. 9, ¶ 4; Richgels Decl., Ex. 10, ¶¶ 2-3; Thompson Decl., Ex. 11, ¶¶ 2-3.

[2]Church Decl., Ex. 2, ¶ 3; Davis Decl., Ex. 3, ¶ 2; Hurd Decl., Ex. 4, ¶ 3; Layton Decl., Ex 1, ¶ 6, 10; Marcynzsyn Decl., Ex. 5, ¶ 4; Mullen Decl., Ex. 6, ¶¶ 2-3; Pritchett Decl., Ex. 7, ¶ 2; Randall Decl., Ex. 8, ¶ 4; Renteria Decl., Ex. 9, ¶ 5; Richgels Decl., Ex. 10, ¶ 2; Thompson Decl., Ex. 11, ¶ 3.

[3]Church Decl., Ex. 2, ¶ 2; Davis Decl., Ex. 3, ¶ 3; Hurd Decl., Ex. 4, ¶ 7; Layton Decl., Ex 1, ¶ 11; Marcynzsyn Decl., Ex. 5, ¶ 4; Mullen Decl., Ex. 6, ¶ 3; Pritchett Decl., Ex. 7, ¶ 3; Randall Decl., Ex. 8, ¶ 4; Renteria Decl., Ex. 9, ¶ 6; Richgels Decl., Ex. 10, ¶ 2; Thompson Decl., Ex. 11, ¶ 3.

[4]Church Decl., Ex. 2, ¶ 2; Davis Decl., Ex. 3, ¶ 2; Hurd Decl., Ex. 4, ¶ 3; Layton Decl., Ex 1, ¶¶ 8 - 9; Marcynzsyn Decl., Ex. 5, ¶ 3; Mullen Decl., Ex. 6, ¶ 2; Pritchett Decl., Ex. 7, ¶ 2; Randall Decl., Ex. 8, ¶ 4; Renteria Decl., Ex. 9, ¶ 6; Thompson Decl., Ex. 11, ¶ 3

XP Antivirus 2008, nothing happened and she never received the product. Id. at ¶ 7. Uncertain about how to proceed, Randall conducted an Internet search for XP Antivirus 2008 and found numerous consumer complaints calling the product a scam. Id. at 8. Randall then called her credit card company to inquire about the charge, but was informed that the charge had already been processed. Id. at ¶ 9. Randall never received a refund or credit. Id.

Several consumers report similar experiences, but report that Defendants' scanner "detected" pornography on their computers rather than viruses. For instance, Kent Woerner, the Network Administrator for Unified School District 273 in Beloit, Kansas, was alerted when a female student using a sixth grade classroom computer was exposed to pornographic images, which were displayed as part of a pop-up advertisement that purported to scan the computer the student was using. Woerner Decl., Ex. 12, ¶¶ 2 - 3. When Woerner consulted the log file history for the computer, he discovered that the Defendants' *advancedcleaner.com* website was the source of the advertisement. Id. at ¶ 5. Woerner proceeded to visit the URL recorded in the log file and witnessed the same scan described by the student, which claimed to detect pornography on his computer and displayed a series of explicit pictures, including an image of a woman performing oral sex. Id. at ¶¶ 6-7. At the conclusion of the scan, the advertisement urged Woerner to purchase AdvancedCleaner to remove the pornography detected on the computer. Id. at ¶ 8. Suspecting that the scan was fake, Woerner searched the computer for the pornographic images purportedly "detected" and found none. Id. at ¶ 9. He then proceeded to visit the same AdvancedCleaner URL from two other school district computers, and received the exact same scan with the exact same results. Id. at ¶ 10. Based on this experience, Woerner concluded that the scan displayed in Defendants' AdvancedCleaner advertising is fake, and consists of nothing more than a movie displayed within the Internet browser. Id. at ¶ 11.

Consumer Joe Renteria relates a similar experience. Renteria observed an unsolicited Internet Explorer window appear on his screen and display a scan of his computer. Renteria Decl., Ex. 9, ¶ 5. The scan showed various pornographic images, and claimed that the images resided on his computer.

Id. At the conclusion of the scan, Renteria was urged to download Defendants' AdvancedCleaner product to remove the pornographic images detected on his computer. Id. at ¶ 6. As an experienced web designer, Renteria recognized the scan as nothing more than an animated image displayed in his web browser and proceeded to file a complaint with one of the FTC's law enforcement partners. Id. at ¶ 7. Within his complaint, Renteria included the URL of the AdvancedCleaner scan that he saw. Id. As discussed below, both FTC investigator Drexler and online advertising industry veteran Michiel Nolet later visited this URL, which is part of the Defendants' *advancedcleaner.com* website. Both Drexler and Nolet saw the exact same bogus system scan reported by Renteria, and have both independently verified Renteria's conclusion that the scan is fraudulent.

B. The FTC's Investigation

Through a variety of investigative techniques, the FTC has established that Defendants market their products to consumers by means of bogus system scans that falsely "detect" the presence of viruses, trojans or pornography on consumers' computers. The FTC has also tied each of the Defendants to these deceptive practices. As discussed in depth below, the FTC's evidence of the Defendants' unlawful scheme is overwhelming and includes Defendants' own admissions, which are contained within the pleadings and affidavits filed in a lawsuit the Defendants are litigating in the Ontario Superior Court of Justice.

1. Defendants' Scans Are Bogus

Defendants market a wide range of security software by displaying to consumers bogus system scans that purport to detect security or privacy violations. At the conclusion of these scans, Defendants urge consumers to purchase their security products to remedy the non-existent problems "detected" in the bogus scan. Defendants market more than one hundred different products in this fashion. Three of the most heavily marketed of these products – AdvancedCleaner, WinAntiVirus and DriveCleaner – are discussed below.

a. Defendants' AdvancedCleaner Scan Falsely Claims To Detect Pornographic Files

AdvancedCleaner is one of many privacy protection products Defendants market and sell to the public. Drexler Decl., Ex. 20, ¶¶ 164 - 169. To market AdvancedCleaner, Defendants rely on advertisements that display an elaborate "internal files scan" that invariably "detects" pornographic files on scanned computers. Id. at ¶¶ 167, 175. By visiting the URL provided to the FTC in the consumer complaint filed by Joe Renteria (see Section III.A, *supra*), FTC Investigator Drexler was able to view and capture the unsolicited AdvancedCleaner advertisement Renteria witnessed on his computer. Id. at ¶¶ 166 - 168. A screenshot of this advertisement appears below[5]:

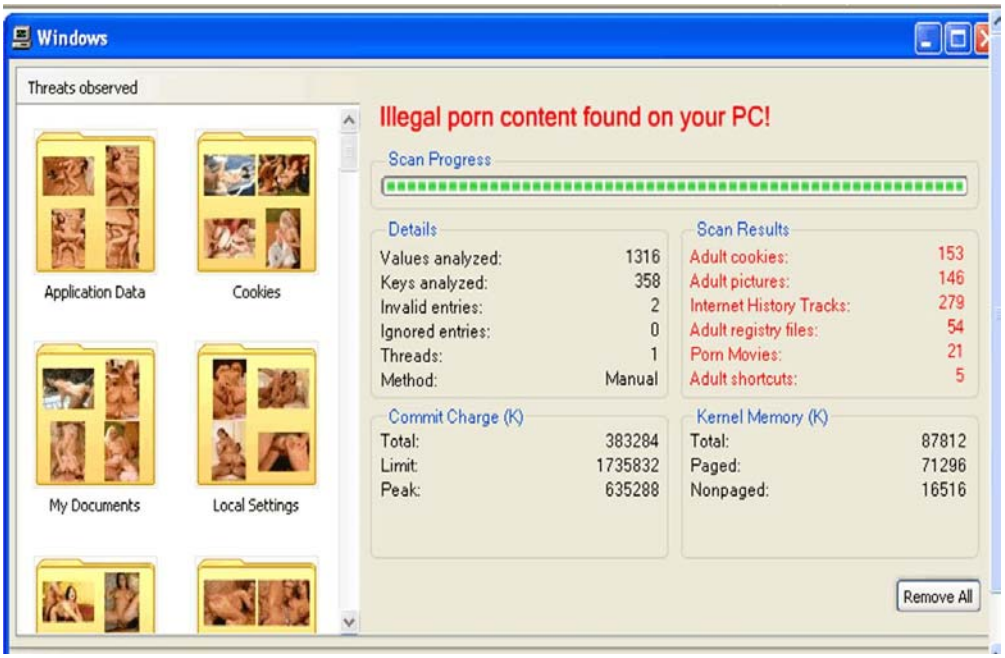

Figure 1

Within this advertisement, Defendants make a series of misrepresentations. First, Defendants claim

[5]Defendants use explicit images to market their products. Because these images are central to the Defendants' deceptive marketing efforts, they have been reproduced without redaction in this memorandum and in the FTC's Complaint. If the Court would prefer that these images be redacted from the publicly-accessible versions of these pleadings, the FTC will provide redacted copies to the clerk's office.

that "[i]llegal porn content" exists on the computer "scanned" by the ad. Second, Defendants display a series of pornographic images under the heading "[t]hreats observed" along with the folder locations where these pictures purportedly reside. Third, Defendants make a variety of claims under the heading "Scan Results," including the representation that the scan detected 21 "Porn Movies" and 146 "Adult Pictures." Each of these representations is false. None of the pornographic pictures purportedly detected in the advertisement actually exist on the "scanned" computer. Drexler Decl., Ex. 20, ¶ 170 - 175. Indeed, the entire "scan" conducted in the Defendants' ad is a ruse that consists of nothing more than a movie displayed in the viewer's Internet browser. Id. at ¶ 174. As a result, the scanner displays the exact same results each time it runs, regardless of which computer the ad is displayed upon. Drexler Id. at ¶ 175. This is true even on the FTC's Internet Lab computers, which are reset before each use to a pristine, "out of the box" state and contain no pornographic files of any kind. Id.

The advertisement pictured above is but one of an arsenal of similar ads that reside on Defendants' *advancedcleaner.com* website. Drexler Decl., Ex. 20, ¶ 169. While these ads differ in appearance, they all rely on the same deceptive marketing technique – false statements about explicit/pornographic content allegedly detected on the "scanned" computer. Id. Many of these ads include photographs of graphic depictions of sexual activities that purportedly exist on the scanned computer. Id. Screenshots of more than 15 of these advertisements are attached to FTC Investigator Drexler's declaration as Attachment II. All of these ads are bogus. Indeed, when viewed from the same computer one after another, the ads contradict each other, and report wildly different numbers of pornographic files "detected" on the exact same computer. Id.

Examples of three of these ads, which were viewed only minutes apart on the same computer, are displayed below. The first AdvancedCleaner ad displays a series of pornographic pictures purportedly found on the scanned computer and informs the viewer that there are "156 pornographic files in your system." The second AdvancedCleaner ad "locates" and displays an entirely different set of explicit pictures and informs the viewer that it detected a total of 44 pornographic files on the scanned computer.

The third advertisement contradicts both of these findings, by "locating" and displaying yet another series of explicit pictures and claiming that 316 "compromising" and "Internet track" files exist on the computer. This same charade plays out over and over again in the more than 15 other AdvancedCleaner advertisements attached to Investigator Drexler's Declaration as Attachment II.

Figure 2

Figure 3

Figure 4

In order to independently confirm that the AdvancedCleaner scans are a ruse, the FTC provided the URL for the AdvancedCleaner ad witnessed by Consumer Joe Renteria (Figure 1) to Michiel Nolet, the former Director of Analytics for online advertising company Right Media. Nolet has extensive experience with malicious electronic advertisements and developed the software used by Right Media to

detect these types of ads. Nolet Decl., Ex. 13, ¶ 3. After reviewing the Defendants' AdvancedCleaner advertisement, Nolet confirmed that the ad consists of nothing more than an Adobe Flash[6] animation, and is incapable of conducting the scan it claims to have completed. Id. at ¶ 8.

At the completion of the fake scans in Defendants' AdvancedCleaner advertisements, Defendants urge consumers to download the AdvancedCleaner program in order to rid their computers of the pornography "detected" by the bogus scanner. Drexler Decl., Ex. 20, ¶¶ 208 - 209. Once AdvancedCleaner is downloaded and installed, Defendants present another bogus scan, which is initiated by the Defendants' software. Id. at ¶ 210. This second scan, an example of which is displayed below, repeats many of the same misrepresentations made in the original advertisement, including this dire warning:

> **216 Adult Content Detected** [*sic*]
> **Your PC has stored 216 items that are dangerous to your reputation . . .**
> **To protect your family/career/property and get rid of these compromising contents, you need to hide them completely by means of AdvancedCleaner. For software registration, please click the "Register Now!" button.**

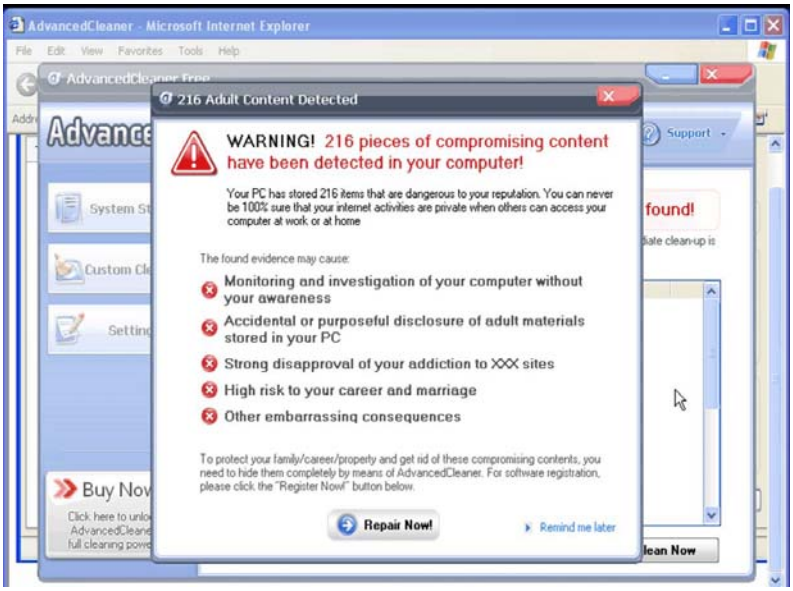

Figure 5

[6] Adobe Flash is multimedia software used to add animation and interactivity to web pages. See http://www.adobe.com/products/flash.

Contrary to the Defendants' explicit representations, the "[a]dult [c]ontent" detected by the Defendants' software-based scanner does not actually exist. Drexler Decl., Ex. 20, ¶ 207 - 211. Nonetheless, Defendants urge consumers to eliminate these adult files from their computers by clicking the "Register Now" button. Id. at ¶¶ 211 - 12. Consumers who follow this instruction are informed that they must register AdvancedCleaner at a cost of $39.95 in order to remove the adult files "detected" by the program. Id. at 212.

b. Defendants' WinAntiVirus Scan Falsely Claims To Detect Computer Viruses

WinAntiVirus is one of many antivirus products marketed by the Defendants. Drexler Decl., Ex. 20, ¶¶ 176 - 186. FTC Investigator Drexler reviewed multiple WinAntiVirus advertisements hosted on the Defendants' *amaena.com* website, which was named in many consumer complaints as one of the sources of Defendants' advertising. Id. at ¶¶ 176 - 81. Each of the WinAntiVirus advertisements hosted on *amaena.com* contains misrepresentations about the security status of the computer on which the ad is displayed. Id. at ¶¶ 176 - 186. One of these ads, pictured below, informs viewers "WARNING: YOUR CURRENT ANTIVIRUS PROTECTION IS NOT EFFECTIVE!" It also states that "your system is currently sending private information and documents to a remote computer."

Figure 6

Consumers who attempt to close this window see another pop-up window with the ominous warning below:

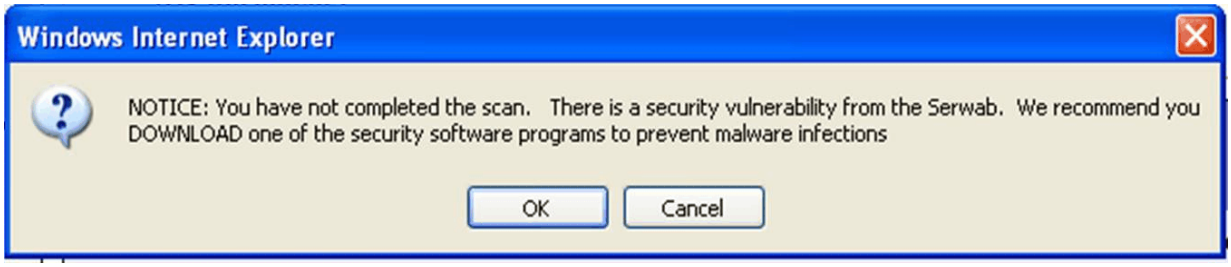

Figure 7

The representations in the advertisement above as well as the followup pop-up window are false. Drexler Decl., Ex. 20, ¶¶ 182- 86. The advertisement detects the same purported vulnerabilities no matter which computer it is displayed upon, including the pristine computers within the FTC's Internet lab. Id. at ¶ 186. Moreover, the warning "YOUR CURRENT ANTIVIRUS IS NOT EFFECTIVE" is displayed even on computers running the latest versions of legitimate antivirus software, including Symantec Antivirus, which is installed on the FTC Internet lab computers used to view the advertisements. Id. at ¶¶ 181, 186.

In addition to their bogus virus scans, several of Defendants' WinAntivirus advertisements misappropriate the "look and feel" of the Microsoft Windows XP Security Center, a program bundled with Microsoft Windows XP that runs automatically and notifies consumers when their security settings put them at risk. Drexler Decl., Ex. 20, ¶ 182. By copying portions of the official Windows XP Security Center – including the "Security Center: Help Protect your PC" logo, the Windows XP Security Center "shield," and the "Resources" list in the left column – Defendants dupe consumers into believing that Windows XP itself has detected a problem with their computer and is urging them to purchase

Defendants' software. Id. at ¶¶ 182 - 83. An example of one of these misleading ads appears below.

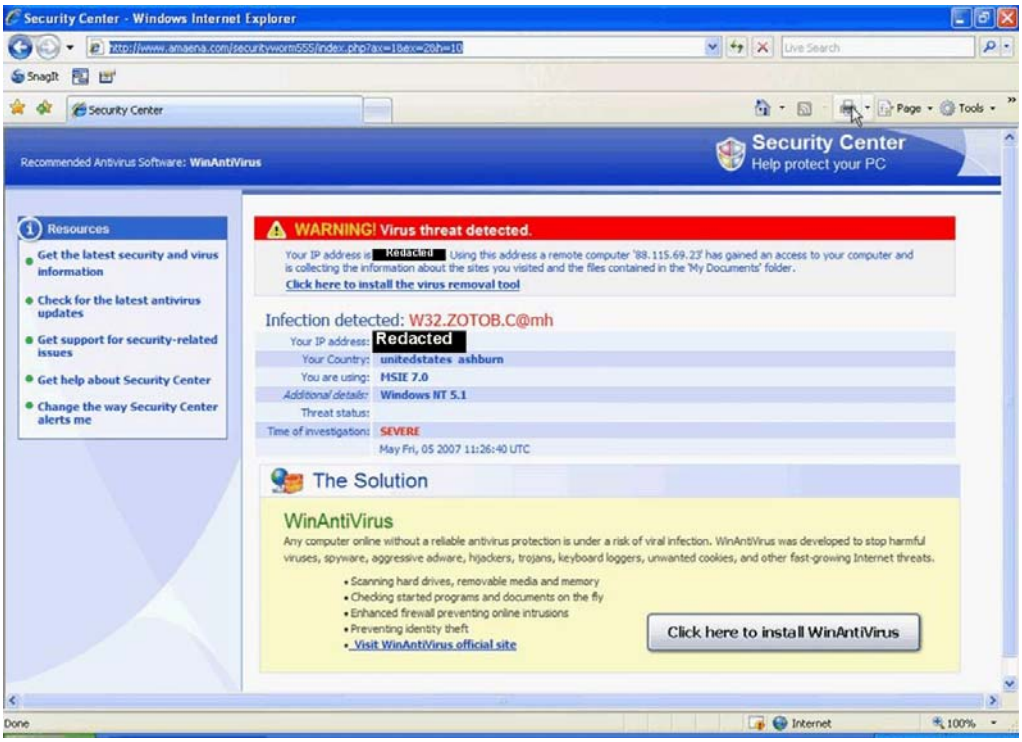

Figure 8

c. Defendants' DriveCleaner Scan Falsely Claims To Detect Dangerous Files

DriveCleaner is another security product marketed by the Defendants through deceptive advertising. Drexler Decl., Ex. 20, ¶¶ 187 - 203. Similar to AdvancedCleaner, DriveCleaner is promoted by Defendants as a product that will "[e]rase all compromising evidence" from consumers' computers. Id. at ¶ 197. By reviewing consumer complaints that include the URL of the DriveCleaner advertisement consumers saw, and by following links posted by a security researcher who has tracked the progression of Defendants' deceptive ads, FTC Investigator Drexler was able to review a series of Defendants' DriveCleaner advertisements that are in wide circulation on the Internet. Id. at ¶¶ 188, 196 - 98. Like the Defendants' AdvancedCleaner ads, Defendants' ads for DriveCleaner purport to scan consumers' computers and detect "Pornographic," "Adult," "Sensitive," or "Compromising" files. Id.

at ¶¶ 197, 199. An example of one such advertisement is pictured below:

Figure 9

Defendants urge consumers who see their DriveCleaner ads to download and purchase the program in order to remove the files detected during the scan. Drexler Decl., Ex. 20, ¶ 190. Once again, all of the representations in Defendants' advertisement are false. Id. at ¶¶ 199, 202 - 03. No actual scan occurred and the ad "detects" the same number of files no matter which computer it runs upon. Id. at ¶ 203.

In other DriveCleaner ads, like the one pictured below, Defendants purport to have detected 179 visits to "Adult websites" and 21 visits to "Illegal websites," including "*getlaid.com*," "*gayanalsex.com*," and "*asianteens.net*." Drexler Decl., Ex. 20, ¶ 194. These representations are false. Drexler Decl., Ex. 20, ¶¶ 200 - 203. No scan has occurred and the "adult" and "illegal" sites displayed

in the ad never change, regardless of which computer the ad is displayed upon, including the pristine computers within the FTC's Internet Lab. Id. at ¶ 203.

Figure 10

2. Defendants Dupe Internet Advertising Networks and Commercial Websites Into Displaying Their Exploitive Ads

Defendants have long relied on advertisements featuring bogus system scans to sell their software. Drexler Decl., Ex. 20, ¶ 123. Until recently, Defendants have been able to freely place these ads directly with major ad networks. Indeed, defendant Kristy Ross was able to place more than $3.3 million worth of advertisements for Defendants' security products with the MyGeek advertising network alone between October 2004 and November 2006. Id. at ¶ 111.

The advertisements placed by Defendant Ross on the MyGeek network quickly drew complaints from MyGeek's advertising partners. Drexler Decl., Ex. 20, ¶ 116 - 17. Advertisers informed MyGeek

that Ross' ads should not be displayed to their users because they were "aggressive and bad ad[s]." Id. at ¶ 116. On multiple occasions, representatives from MyGeek chastised Defendant Ross for placing advertisements that violated MyGeek guidelines, including ads that contained "auto-downloads" – advertisements that attempted to install the Defendants' software without consumer consent – and ads that forced users to view Defendants' websites. Id. at ¶ 115. Although Ross promised to fix the offending ads, and claimed that these ads were mistakes, all such "fixes" proved temporary. Id. In March 2007, MyGeek ended its relationship with the Defendants, and informed Ross via email that it would no longer accept advertising for any of Defendants' security products. Id. at ¶ 118.

With major advertising networks like MyGeek refusing to accept Defendants' advertisements, Defendants were forced to alter their tactics and begin to dupe advertising networks and commercial websites into accepting their advertising. In furtherance of this scheme, Defendants have created a number of sham Internet advertising agencies to place advertisements for the Defendants' products. Drexler Decl., Ex. 20, ¶ 150. These captive advertising agencies, including "ForceUp," "Burn Ads," "AdTraff," "NetMediaGroup," and "Uniqads," approach popular advertising networks and commercial websites offering to purchase advertising space on behalf of legitimate companies. Drexler Decl., Ex. 20, ¶ 161; Cohen Decl., Ex. 14, ¶¶ 4 - 13. Although these legitimate companies have no affiliation with Defendants, and have never authorized Defendants to place advertising on their behalf, the Defendants falsely represent that they are authorized to place the advertisements. Id. at ¶¶ 4 - 13.

The Defendants then supply the targeted advertising network or website with a technologically sophisticated electronic advertisement or "creative," which is capable of displaying different content depending on a variety of criteria, including the Internet Protocol ("IP") address of the viewer. Nolet Decl., Ex. 13, ¶ 7. When this creative is viewed from a computer with an IP address associated with the advertising network or website upon which they are advertising, or any other IP range chosen by the Defendants, the advertisement appears as promised – as a banner ad for the legitimate company or organization Defendants claim to represent. Id. at ¶¶ 6 - 7. As a result, when the advertising staff of

the targeted advertising network or website views the ad, they see nothing unusual and proceed to approve the Defendants' ad for distribution.

However, due to hidden programming code inserted by the Defendants, the Defendants' advertisements appear entirely differently to those outside of this "walled off" IP range. Nolet Decl., Ex. 13, ¶ 7; Cohen Decl., Ex. 14, ¶¶ 7 - 8. Consumers with an IP address outside of the IP range walled off by the Defendants receive an exploitive ad that takes them from the website they are visiting to one of the Defendants' websites. Cohen Decl., Ex. 14, ¶¶ 7 - 8. At this point, one of the Defendants' fake scans commences and proceeds to "detect" a host of critical threats that can be resolved by purchasing Defendants' software. Id. at ¶¶ 7 - 8.

The popular Internet site *zillow.com* is among the websites that have fallen victim to the Defendants' tactics. In mid-November 2007, one of Defendants' sham ad agencies – NetMediaGroup – contacted Zillow about running ads for online travel website *skyauction.com*. Cohen Decl., Ex. 14, ¶ 4 The NetMediaGroup advertising campaign for SkyAuction began running on *zillow.com* on December 1, 2007. Id. at ¶ 6. By December 4, 2007, Zillow became aware of reports from its customers that they were being redirected away from *zillow.com* to a different and unaffiliated "malware pop up" website where Zillow customers were exposed to one of the Defendants' fake scans. Id. at ¶ 7

Zillow investigated the customer complaints and determined that the SkyAuction advertisements placed by NetMediaGroup were responsible for redirecting customers away from *zillow.com*. Cohen Decl., Ex. 14 at ¶ 8. On December 5, 2007, Zillow notified NetMediaGroup of the complaints associated with its advertising campaign and requested NetMediaGroup's signed agreement with SkyAuction. Id. at ¶ 9. In response, NetMediaGroup provided an undated "Letter of Mandate" that stated "I hereby confirm that NetMediaGroup advertising agency is permitted to promote Skyauction.com[tm] services." Id. at ¶ 10. The letter appeared to be printed on SkyAuction letterhead and was signed by Michael N. Hering, the President and Chief Executive Officer of SkyAuction.com, Inc. Id. at ¶ 10. On December 6, 2007, Zillow contacted SkyAuction and spoke directly with Michael

Hering and with Gary Doughty, the CTO of SkyAuction. Id. at ¶ 11. During this conversation, Zillow learned that SkyAuction was neither aware of, nor had any relationship with, NetMediaGroup. Id. Zillow informed NetMediaGroup about its conversation with SkyAuction and terminated its contract with NetMediaGroup. Id. at ¶ 12. Upon being informed of the contract termination, NetMediaGroup responded with an email stating: "What can I say…? It was worth a try." Id. at ¶ 13.

Zillow is not the only website to be victimized by Defendants' exploitive advertising. Since 2007, Defendants have succeeded in deceiving a number of popular Internet websites into running their exploitive ads, including the websites for Major League Baseball (*mlb.com*), the National Hockey League (*nhl.com*), The Economist magazine (*economist.com*), the National Association of Realtors (*realtor.com*), and the popular Internet dating site E-Harmony (*eharmony.com*). Drexler Decl., Ex. 20, ¶ 160.

3. Each Defendant Has Played a Crucial Role in this Scam

Despite extensive efforts by the Defendants to hide from law enforcement, multiple, independent sources of evidence establish their respective roles in the enterprise. Among the most compelling of this evidence are pleadings and affidavits filed in a lawsuit currently pending in the Ontario Superior Court of Justice (the "Canadian lawsuit"). See Wilcock Decl., Ex. 15; Moriarity Decl., Ex. 16.

Filed by Innovative Marketing at the behest of Defendants Sam Jain and Daniel Sundin, the Canadian lawsuit alleges that defendant Marc D'Souza and relief defendant Maurice D'Souza embezzled $48 million from Innovative Marketing between 2002 and 2006. See Statement of Claim, attached to Christopher Decl., Ex. 17 as Attach. A. Based on the allegations in the complaint, the Ontario Superior Court entered a Mareva injunction freezing more than $40 million in assets belonging to Marc and Maurice D'Souza.[7] See Order dated May 2, 2007, attached to Christopher Decl., Ex. 17 as Attach. E. In

[7]Days before filing this suit, we learned that the Mareva injunction in the Canadian litigation was lifted at the request of the parties on November 4, 2008, and the frozen funds distributed to accounts around the world pursuant to a settlement between the parties.

response, Marc D'Souza filed a counterclaim against Innovative Marketing, Jain, and Sundin, alleging breach of fiduciary duty. See Statement of Defence and Counterclaim, attached to Christopher Decl., Ex. 17, Attach. B. The pleadings and affidavits filed in the case contain a series of admissions that confirm the allegations in the FTC's Complaint, tie each of the Defendants to the scheme, and identify many of the products Defendants have deceptively marketed to consumers around the world.

i. Innovative Marketing, Inc.

Innovative Marketing, Inc. ("IMI") is the corporate entity used by the Defendants to market and sell their products. Drexler Decl., Ex. 20, ¶¶ 34; 38 - 47; 54 - 64. Innovative Marketing was incorporated by defendant Daniel Sundin in July 2002, and is listed as the registrant of several of the Defendants' software security product websites, including *drivecleaner.com* and *winantivirus.com*. Id. at ¶ 34 and Attach. A. Pleadings and affidavits from the Canadian lawsuit confirm that defendants Ross, Sundin, and Jain serve as officers of Innovative Marketing and that defendant Marc D'Souza was an officer until his departure in late 2006. See Drexler Decl., Ex. 20, at ¶¶ 34, 98, 107, 122, 124. The Canadian lawsuit also confirms that Innovative Marketing is the entity that markets Defendants' security products, including WinFixer, DriveCleaner, WinAntiVirus, SystemDoctor, ErrorSafe, and many others. Christopher Decl., Ex. 17, Attach. A at ¶ 19 and Attach. B at ¶¶ 46, 171. Between 2004 and 2006, Innovative Marketing reported gross profits of more than $92 million. Christopher Decl., Ex. 17, Attach. M at Ex. A.

Although Defendants operate through the incorporated entity Innovative Marketing, they fail to observe most corporate formalities. Drexler Decl., Ex. 20, ¶ 139 - 142. Defendants utilize a variety of shell companies and aliases, deliberately maintain few records of their business activities, and operate without a written agreement delineating their roles and responsibilities. Id. at ¶¶ 139 - 142; 152.

ii. ByteHosting Internet Service, LLC

ByteHosting is owned by Defendant James Reno, and operates as a common enterprise with IMI. Defendants refer to ByteHosting as the "Ohio office" of IMI, and virtually all of ByteHosting's revenue is received from IMI's accounts. Drexler Decl., Ex. 20 at ¶¶ 92-3. On numerous occasions, IMI wired funds to ByteHosting for the express purposes of paying payroll, rent, taxes, and utilities. Id. at ¶¶ 95-6. Hereinafter, IMI and ByteHosting are referred to as the "IMI Enterprise."

Defendants Reno and ByteHosting perform a variety of functions for IMI that perpetuate the Defendants' scheme to defraud consumers, including the operation of a "customer support" call center that fields inquiries from consumers who have purchased Defendants' products. Drexler Decl., Ex. 20, ¶ 78, 82. Call center staff routinely obstruct or delay consumers seeking refunds after they have purchased Defendants' products. Id. at ¶¶ 26, 75.

Phone numbers that belong to ByteHosting and James Reno are utilized by Defendants in connection with the sale of their products. Drexler Decl., Ex. 20, ¶ 71. Several of the merchant identifiers consumers see on their credit card statements after they purchase Defendants' security products contain a phone number that belongs to James Reno. Id. at ¶¶ 56 - 58. For example, consumers purchasing Defendants' AdvancedCleaner product see "supportsw.com 8007555509" as the merchant identifier. Id. at ¶ 57. This toll free phone number belongs to Reno. Id. at ¶ 71. Moreover, several of the customer support telephone numbers Defendants provide to purchasers of their software belong to Reno. Id.

iii Daniel Sundin

Defendant Daniel Sundin is the former Chief Operating Officer and current Chief Technology Officer of IMI, and is also the "chief designer" of the IMI Enterprise's security products. Drexler Decl., Ex. 20, ¶¶ 34, 36. Sundin is also the President of Vantage Software, which is the entity responsible for procuring hundreds of the domain names used by the Defendants, including *innovativemarketing.com*, *winantivirus.com*, *drivecleaner.com*, among many others. Id. at ¶¶ 38, 40. In the Canadian lawsuit, Sundin filed an affidavit that includes a description of how DriveCleaner is marketed to consumers. Christopher Decl. Ex. 17, Attach. G at ¶ 13, and Ex. D. This affidavit includes a screenshot of a

DriveCleaner advertisement that is substantively identical to the bogus scan advertisement discussed in Section III.B(1)(c) of this memorandum. Id. Sundin also used his personal credit card to pay for Defendants' product advertisements placed with online advertising network MyGeek. Id.

iv. Sam Jain

Defendant Sam Jain is the Chief Executive Officer of IMI, and has overseen the IMI Enterprise's operations since 2002. Drexler Decl., Ex. 20, ¶ 98. Jain is also responsible for bringing his former girlfriend, Kristy Ross, and his long time business associate, James Reno, into the company. Id. at ¶ 98, 104. Jain acknowledges his day-to-day control over the operations of the IMI Enterprise in an affidavit filed in the Canadian lawsuit, in which he states that any expenditure of IMI's resources must be approved by both Sundin and himself. Christopher Decl., Ex. 17, Attach. F at ¶ 63.

In 2004, Jain was sued by Symantec Corporation, along with his business partner James Reno, for pirating Symantec's security software. Drexler Decl., Ex. 20, ¶ 102. Jain evaded service of the complaint and a default judgment was entered against him. Id. Although Jain later moved to overturn the default judgment, the Court denied the request, finding that Jain had "cynical[ly] and intentional[ly] manipulat[ed]" the proceedings by evading service of Symantec's complaint. Id.

v. Marc D'Souza

Marc D'Souza was a senior executive with IMI until late 2006, when he split from the company. Drexler Decl., Ex. 20, ¶ 122, 124. D'Souza functioned as Chief Financial Officer and Chief Marketing Officer of IMI, and was responsible for developing relationships with payment processors that could process the huge volume of sales generated by the company. Id. at ¶ 124. D'Souza's role was especially important, since the IMI Enterprise has great difficulty maintaining relationships with payment processors due to the high rate of chargebacks and complaints from defrauded consumers. Id. at ¶ 125. D'Souza's central role in the IMI Enterprise's billing operations is further evidenced by his ownership of Synergy Software, B.V., the company that controls several of the merchant accounts used by the Defendants to bill consumers for their products. Id. at ¶ 127. Marc D'Souza, along with his

father Maurice D'Souza, holds tens of millions of dollars in proceeds from IMI's operations in his bank accounts. Id. at ¶ 131.

In the Canadian pleadings, Marc D'Souza takes credit for developing the "scanner approach" used to sell Defendants' software, and states that it was he who convinced defendant Jain to adopt the "scanner approach" in order to market Defendants' software. Drexler Decl., Ex. 20, ¶ 123.

vi. Kristy Ross

Defendant Kristy Ross is the Vice President of Business Development for IMI and is primarily responsible for marketing Defendants' products. Drexler Decl., Ex. 20, ¶ 107. Ross placed millions of dollars in deceptive advertising for Defendants' products, including WinFixer, ErrorProtector, WinAntivirus, DriveCleaner, ErrorSafe, and SystemDoctor. Id. at ¶¶ 110-11. As demonstrated by her cell phone records, Ross is in routine contact with her co-Defendants, including both James Reno and Marc D'Souza. Id. at ¶ 113. Recently, Ross appears to have taken a more senior role with IMI. According to an affidavit filed by defendant Sundin in the Canadian litigation, Ross has assumed some of the duties of IMI Chief Technology Officer while Sundin battles an extended illness. Christopher Decl., Ex. 17, Attach. I at ¶ 15.

As discussed in more detail in Section III.B(2), on multiple occasions the ads Ross placed for Defendants' products were found to act in a malicious fashion, by attempting auto-downloads and by forcing consumers to view Defendants' websites. Ross also told MyGeek that she could ensure that Defendants' software would not detect the "adware" (advertising software installed by third-parties on consumers' computers, often without consent) used by MyGeek's partners to display ads on consumers' computers. Drexler Decl., Ex. 20, ¶ 117.

vii. James Reno

Defendant James Reno is a long time business associate of defendant Jain, and was sued along with Jain by Symantec Corporation in 2004 for pirating Symantec's software. Drexler Decl., Ex. 20, ¶¶ 85, 102. Reno has advanced computer skills and has played an important role in furthering Defendants'

scheme. Id. at ¶ 68. Among other responsibilities, Reno runs the Defendants' call center, purchases and maintains computer equipment for the IMI Enterprise, and manages key contracts on Defendants' behalf, including the critical content delivery contract with LimeLight Networks, which allowed Defendants to disseminate their advertising and software to consumers around the world. Id. at ¶¶ 71, 78, 82. Reno is also connected to at least one of the sham advertising agencies used by the Defendants, as well as "SetUpAHost, Inc.," one of the shell companies used extensively by Defendants. Id. at ¶¶ 86 - 90, 147. In 2006, Reno was named as a defendant in a private lawsuit filed in California. Id. at ¶ 69. The lawsuit accused Reno of being one of the masterminds of Defendants' "fraudware" products, including WinFixer and WinAntiVirus. Id.

viii. Maurice D'Souza

Maurice D'Souza was directly involved in setting up the various merchant accounts the IMI Enterprise used to process consumer payments. Drexler Decl., Ex. 20, ¶ 134 - 36. Although Maurice D'Souza has no contract or other compensation agreement with the IMI Enterprise, at least $18.5 million of the IMI Enterprise's assets reside in his personal and corporate bank accounts. Id. at ¶ 130.

C. The Internet Security and Online Advertising Communities Have Declared Defendants' Tactics a Significant Threat To Internet Users

The Defendants' deceptive marketing tactics have drawn the attention of both the computer security and online advertising communities, which have cited Defendants' software – and the deceptive manner in which it is marketed – as a grave threat to Internet users.

Every major computer security company, including Symantec Corp., Microsoft Corp., Kaspersky, PCTools, Panda Software, Sunbelt Software, Inc., Computer Associates, F-Secure, McAfee, Inc., ParetoLogic, Sophos PLC, and Tenebril, Inc. has declared the Defendants' products a threat to consumers. Drexler Decl., Ex. 20, ¶ 30. For example, PCTools describes Defendants' ErrorSafe product as a "rogue anti-spyware program which pretends to scan your computer and show severe system threats installed on it. After that it prompts you to buy this software." Id. at Attachment C at

173. Symantec notes that Defendants' AdvancedCleaner program purports to scan computers and "then reports a number of false threats." Id. at 191. In addition, both Google and McAfee list several of the Defendants' webpages as harmful, and urge consumers not to visit them. Drexler Decl., Ex. 20, ¶¶ 39, 41.

StopBadWare.Org, a project of Harvard Law School's Berkman Center for Internet & Society, tested several of Defendants' products and declared them unsafe and deceptively marketed. Drexler Decl., Ex. 20, ¶ 31. For example, the StopBadWare.org report on Defendants' DriveCleaner program notes that the program is sold utilizing "fear tactics," including false pop-up ads that mimic legitimate system warnings and purport to detect a large number of non-existent "dangerous" or "compromising" files. Id. StopBadWare.Org has made similar findings about Defendants' WinFixer, WinAntiSpyware, WinAntiVirus, XP AntiVirus 2008, and PerformanceOptimzer products. Id.

The online advertising community has also sounded the alarm about Defendants' tactics. As discussed earlier, Michiel Nolet is an online advertising industry veteran. While employed at Right Media, Nolet first observed Defendants' products advertised through sophisticated electronic advertisements that purport to promote legitimate products, but contain hidden code capable of redirecting consumers to the Defendants' websites, including *errorsafe.com*, *drivecleaner.com*, and *systemdoctor.com*. Nolet Decl., Ex. 13, ¶¶ 3, 6-7. Nolet maintains a website where he authors articles about online advertising. On this website, Nolet has posted more than 25 different versions of the Defendants' exploitive ads within a subdirectory entitled "What is errorsafe and how do we stop it?" Id. at ¶ 6. While these ads purport to promote a variety of legitimate companies, including *travelocity.com*, *priceline.com*, and *weightwatchers.com*, they all contain malicious code capable of involuntarily redirecting users to third-party websites, including *errorsafe.com*, *drivecleaner.com*, and *systemdoctor.com*. Id.

D. Defendants' Attempts To Conceal Their Unlawful Activities

The Defendants have gone to extraordinary lengths to conceal their unlawful activities and to hide from law enforcement and defrauded consumers. These efforts are discussed in detail in the Counterclaim filed in the Canadian lawsuit by Defendant Marc D'Souza. Christopher Decl., Ex. 17, Attach. B at ¶ 107. In the Counterclaim, D'Souza discusses how Defendants use "fictitious or misleading vendor names," and notes that "in many cases the Business' products and services themselves were claimed to be owned by fake companies in the name of the product itself." Id.

D'Souza also discusses the Defendants' corporate policy of providing uniformly false domain registration information for their websites:

> [D]omain registration information was modified to conceal the identity of the true operators of the Business. In addition, domain registration information was frequently changed to confuse the public and shield the Business from liability. In fact as the Business grew, detailed policies were established to provide maximum anonymity in the registration, operation and administration of the Business' domains. The domains themselves were used for a short period of time and then discarded or abandoned when there were too many customer complaints or complaints from individuals and security companies who encountered the aggressive or misleading advertising.

Christopher Decl., Ex. 17, Attach. B at ¶ 107.

D'Souza further acknowledges that Defendants use a "variety of different e-mail accounts, a variety of identities, (some real, some fake) and bank accounts in order to confuse and misdirect customers, suppliers and vendors" and use "third party trademarks or likeness to confuse consumers into misidentifying the source of the product." Id.

Finally, D'Souza acknowledges that the Defendants moved the bulk of their operations outside of the United States in order to "escape regulation from the Federal Trade Commission and avoid State Attorneys who were sanctioning and shutting down similar organizations, as well as other civil liabilities from tens of thousands of dissatisfied end consumers." Christopher Decl., Ex. 17, Attach. B at ¶ 125.

The admissions in D'Souza's Counterclaim are consistent with the FTC's experience in attempting to

locate the Defendants and tie them to their unlawful activities. During her investigation, Investigator Drexler routinely encountered false domain registrations, fake company names, shell companies used to bill consumers, bogus or anonymous email addresses, non-existent contact information, and misleading advertising that misappropriates the "look and feel" of Microsoft Windows in order to trick consumers into purchasing Defendants' products. Drexler Decl., Ex. 20, ¶¶ 143 - 146, 150, 154, 156 - 57.

III. ARGUMENT

A. The FTC Act Authorizes the Requested Relief

"Section 13(b) of the Federal Trade Commission Act authorizes the FTC to seek, and the district courts to grant, preliminary and permanent injunctions against practices that violate any of the laws enforced by the Commission." FTC v. Gem Merchandising Corp., 87 F.3d 466, 468 (11th Cir. 1996); FTC v. Ameridebt, 373 F. Supp. 2d 558, 562 (D. Md. 2005). "[B]ecause the district court has the power to issue a permanent injunction to enjoin acts or practices that violate the law enforced by the Commission, it also has authority to grant whatever preliminary injunctions are justified by the usual equitable standards ...." FTC v. H.N. Singer, Inc., 668 F.2d 1107, 1111-13 (9th Cir. 1982); see also Gem Merch., 87 F.3d at 468; FTC v. World Travel Vacation Brokers, 861 F.2d 1020 (7th Cir. 1988). The authority to grant such relief includes the power to grant ancillary relief necessary to accomplish complete justice, including ordering equitable relief for consumer redress. Ameridebt, 373 F. Supp. 2d at 563 (citing FTC v. Febre, 1996 U.S.Dist. LEXIS 9487, *13 (N.D. Ill. 1996), aff'd, 128 F.3d 530 (7th Cir. 1997)). Thus, in addition to injunctive relief, Section 13(b) gives the Court authority to grant any ancillary relief necessary to accomplish complete justice and preserve assets for rescission and restitution. Singer, 668 F.2d at 1112-14; Ameridebt, 373 F. Supp. 2d at 563. This ancillary relief can include freezing assets and expediting discovery. See Gem Merch., 87 F.3d at 468. Other courts in this district and throughout the Fourth Circuit have granted the FTC such preliminary relief.[8]

[8]See, eg., FTC v. Nwaigwe, Civ. No. HAR 96-2690 (D. Md. Aug. 28, 1996) (ordering *ex parte* temporary restraining order with asset freeze and expedited discovery); FTC v.

In determining whether to grant a preliminary injunction under section 13(b), "'a court must 1) determine the likelihood that the Commission will ultimately succeed on the merits and 2) balance the equities.'" World Travel, 861 F.2d at 1029 (citing FTC v. Warner Communications, Inc., 742 F.2d 1156, 1160 (9th Cir. 1984) (per curiam)); FTC v. World Wide Factors, Ltd., 882 F.2d 344, 346-47 (9th Cir. 1989); Ameridebt, 373 F. Supp. 2d at 563. Unlike private litigants, the Commission need not prove irreparable injury, because "harm to the public interest is presumed." World Wide Factors, 882 F.2d at 346; Ameridebt, 373 F. Supp. 2d at 563; Kemp v. Peterson, 940 F.2d 110, 113 (4th Cir. 1991) (upholding preliminary injunction in a HUD statutory enforcement action "since the court determined that the Secretary [of HUD] met his burden of showing violations of the Act . . . as well as a 'reasonable likelihood' of continued violations").

As set forth below, in this memorandum and its five volumes of exhibits, the Commission has presented ample evidence that it will ultimately succeed on the merits and that the balance of the equities favors the requested injunctive relief.[9]

Commercial Electric Supply, Inc., No. WMN 96-1892 (D. Md. June 26, 1996) (ordering *ex parte* temporary restraining order with asset freeze, appointment of receiver, expedited discovery, and immediate access to the premises); FTC v. Premier-Escrow.com, Civ. No. 03-488-A (E.D. Va. Apr. 21, 2003) (ordering *ex parte* temporary restraining order with asset freeze and expedited discovery); FTC v. Tungsten Group, Civ. No. 01-CV-773 (E.D. Va. Oct. 15, 2001) (ordering *ex parte* temporary restraining order with asset freeze, appointment of a receiver, immediate access to premises, and expedited discovery); FTC v. Pereira, Civ. No. 99-1367-A (E.D. Va. Sept. 14, 1999) (ordering *ex parte* temporary restraining order and expedited discovery); FTC v. S.J.A. Society, Inc., No. 97-CV-472 (E.D. Va. May 12, 1997) (ordering *ex parte* temporary restraining order with asset freeze, immediate access to premises, appointment of receiver, and expedited discovery); FTC v. Global Patent Research Servs., Inc., No. 96-676-A (E.D. Va. May 17, 1996) (ordering *ex parte* temporary restraining order with asset freeze, immediate access to premises, and expedited discovery); FTC v. Independence Medical, Inc., No. 2-95-1581-18 (D. S.C. May 22, 1995) (ordering *ex parte* temporary restraining order with asset freeze, appointment of a temporary receiver, immediate access to financial records, and expedited discovery).

[9]Although not required to do so, the Commission also meets the Fourth Circuit's four-part test for private litigants to obtain injunctive relief as set forth in Blackwelder Furniture Co. v. Seilig Mfg. Co., 550 F.2d 189,194 (4th Cir. 1977). Without the requested relief, the public and

B. The Commission Will Likely Succeed in Demonstrating that the Defendants Have Violated the FTC Act

In order to prevail on its claim that Defendants have violated Section 5 of the FTC Act through deceptive acts or practices, the FTC must establish that "(1) there was a representation, (2) the representation was likely to mislead customers acting reasonably under the circumstances, and (3) the representation was material." FTC v. Tashman, 318 F.3d 1273, 1277 (11th Cir. 2003); FTC v. Pantron I Corp., 33 F.3d 1088, 1095 (9th Cir. 1994) (quoting and adopting standard set forth in Cliffdale Assocs., 103 F.T.C. 110, 164-65 (1984)). Both express claims and implied claims that are false or misleading are actionable under Section 5. FTC v. Figgie Int'l, Inc., 994 F.2d 595, 604 (9th Cir. 1993) (per curiam) (There is "nothing in statute or case law which protects from liability those who merely imply their deceptive claims; there is no such loophole."). The FTC need not prove that the misrepresentations or omissions were done with an intent to deceive. World Travel, 861 F.2d at 1029 ("'[A]n advertiser's good faith does not immunize it from responsibility for its misrepresentations ....'" (quoting Chrysler Corp. v. FTC, 561 F.2d 357, 363 n.5 (D.C. Cir. 1977)); Cliffdale Assocs, 103 F.T.C. at 164-65, appeal dismissed sub nom. Nor does the FTC need to prove reliance by each consumer misled by the defendants. Figgie Int'l, Inc., 994 F.2d at 605-06. Rather, a "presumption of actual reliance arises once the Commission has proved that the defendant made material misrepresentations, that they were widely disseminated, and that consumers purchased the defendant's product." Id.

A misrepresentation is material if it involves facts that a reasonable person would consider important in choosing a course of action. See Kraft, Inc. v. FTC, 970 F.2d 311, 322 (7th Cir. 1992) (quoting Cliffdale Assocs., 103 F.T.C. at 165)) ("A claim is considered material if it 'involves information that is important to consumers and, hence, likely to affect their choice of, or conduct regarding a product.'"); see also Figgie Int'l, 994 F.2d at 603-04; FTC v. Cyberspace.com, LLC, 453 F.

---

the Commission will suffer irreparable harm from the continuation of Defendants' scheme and the likely destruction of evidence and dissipation of assets.

3d 1196, 1201 (9th Cir. 2006). Certain categories of information are presumptively material. For example, express claims, or deliberately made implied claims, used to induce the purchase of a particular product or service, are presumed to be material. See Pantron I Corp., 33 F.3d at 1095-96; Thompson Medical Co., Inc., 104 F.T.C. 648, 373 (1984), aff'd, 791 F.2d 189 (D.C. Cir. 1986).

Here, Defendants engage in deception by: (1) falsely claiming that they have conducted scans of consumers' computers; and (2) falsely claiming that the scans detected a variety of security or privacy threats on consumers' computers. Defendants display advertisements on consumers' computers that appear to be scanning for security or privacy threats. Although Defendants go to great lengths to make these scans appear legitimate, the scans are nothing more than a series of animated graphics. No bona fide scan is ever performed. At the completion of these fake scans, Defendants represent that their scanner has detected a host of urgent security and/or privacy problems, including viruses, spyware, and pornography. In many cases, these false representations are repeated in a software-based scan that Defendants display to consumers after their products are downloaded to consumers' computers.

The bogus scans used by Defendants to market their security products are likely to mislead consumers acting reasonably under the circumstances. Defendants' bogus scans are carefully crafted to mimic legitimate security products and, in many cases, give consumers the impression that the scans they see are generated by their operating systems. See Section III.B(1), *supra*. Given this level of sophistication and trickery – and the massive number of consumers who have purchased the Defendants' security products after viewing these advertisements – there can be no doubt that Defendants' advertising is likely to mislead reasonable consumers.

It also is irrefutable that the false representations made by Defendants are material. The representations within the Defendants' bogus scans are express claims made by the Defendants to induce consumers to purchase their products. As a result, these claims are presumptively material. See Thompson Medical, 104 F.T.C. at 816; Pantron I Corp., 33 F.3d at 1095. Moreover, the fact that Defendants' scans are a fraud, and do not actually detect the critical security or privacy threats

Defendants' claim, is undoubtedly material, since it is information a reasonable person would consider important in deciding whether to purchase Defendants' software. See Kraft, 970 F.2d at 324 (claims exaggerating calcium levels in Kraft Singles affected consumers' purchasing decisions and were material); Figgie Int'l, 994 F.2d at 603-04 (Defendant's failure to inform consumers that smoke detectors provide earlier warnings than the heat detectors sold by the defendant was material, since it was the "single most useful piece of information" consumers could have used). Indeed, it is difficult to imagine a consumer who would buy the Defendants' security software if informed, prior to the purchase, that the scan which led him or her to buy Defendants' product was a fraud.

C. The Balance of Equities Tips Decidedly In the Commission's Favor and Supports Awarding the Requested Injunctive Relief

The balance of the equities tips decidedly in the Commission's favor. Where, as here, public and private equities are at issue, public equities far outweigh private equities. See World Travel, 861 F.2d at 1028-29; World Wide Factors, 882 F.2d at 347; cf. Food Town Stores, 539 F.2d 1339,1346 (4th Cir. 1976) (in a case in which the FTC sought a permanent injunction pending resolution of an administrative complaint, private injuries were "not proper consideration for granting or withholding injunctive relief under § 13(b)"). This is true, in part, because Defendants "can have no vested interest in a business activity found to be illegal." United States v. Diapulse Corp. of Am., 457 F.2d 25, 29 (2d Cir. 1972) (internal quotations and citations omitted).

Here, without the entry of the requested preliminary injunctive relief set forth in the FTC's proposed TRO filed concurrently, the Defendants will continue to engage in their deceptive Internet marketing practices and injure the public during the pendency of the litigation. Defendants have been in business for more than five years and have engaged in the same deceptive practices unabated even in the face of consumer complaints, media attention, and private lawsuits.[10] See Section III.D, *supra*. Further,

[10]In addition, Jain, Reno and D'Souza are not new to this type of fraudulent business scheme. All three were involved in marketing pirated Symantec security software through a business called PMMCI. Jain, Reno and ByteHosting were later sued by Symantec as a result of

it is evident that Defendants can effortlessly add or change, at their will, the products they pitch and the way in which they advertise them. In addition, as described below, Defendants have undertaken substantial efforts to shield their identities in an intentional effort to evade both law enforcement and defrauded consumers. Id. Taken together, these facts weigh strongly in favor of granting the requested injunctive relief.

D. The FTC Has Established That Preliminary Injunctive Relief Is Warranted

Having established that Defendants made representations likely to mislead consumers acting reasonably under the circumstances and that the balance of equities favors the Commission, the FTC has made the showing required to obtain preliminary injunctive relief against the Defendants. In issuing such an order, this Court would join several others that have granted the FTC similar relief based on nearly identical facts.

Although Defendants have introduced a new level of sophistication, scope, and skullduggery, they are operating a familiar Internet scam. For many years, high-tech scam artists have used advertisements featuring bogus system scans to dupe consumers into purchasing their software. The FTC has brought several of these so-called "scareware" cases, including FTC v. MaxTheater, Inc., Civ. No. 05-CV-0069-LRS (E.D. Wash. 2005) and FTC v. Trustsoft, Inc. Civ. No. H-05-1905 (S.D. Tex. 2005). Although the bogus advertisements in these previous cases were neither as aggressive nor sophisticated as the Defendants' advertisements, the courts hearing these cases entered *ex parte* TROs in the FTC's favor in order to immediately halt the unlawful conduct, prevent destruction of documents and, in the case of Trustsoft, prevent dissipation of assets.[11] Given the facts present in this case, this Court should rule similarly.

IV. INDIVIDUAL AND COMMON ENTERPRISE LIABILITY

---

this conduct. See Section III.B(3)(iv), *supra*.

[11]The FTC did not seek an asset freeze in MaxTheater.

Individual defendants, James Reno, Sam Jain, Daniel Sundin, Marc D'Souza, and Kristy Ross, are each liable for violating Section 5 of the FTC Act. Moreover, the corporate defendants, IMI and ByteHosting, operate as a common enterprise, and are therefore liable for each other's violations of Section 5. Furthermore, Maurice D'Souza is liable for equitable relief as a relief defendant.

A. Individual Liability

Once the Commission establishes that a business entity has violated Section 5 of the FTC Act, individual defendants are personally liable for injunctive relief for the business entities' deceptive acts or practices if the individual defendants (1) participated directly in the wrongful practices or acts or (2) had authority to control a corporation engaging in them. FTC v. Freecom Commc'ns., Inc., 401 F.3d 1192, 1202-03 (10th Cir. 2005); FTC v. Publishing Clearing House, Inc., 104 F.3d 1168, 1170 (9th Cir. 1998). Authority to control the company can be evidenced by active involvement in business affairs and making corporate policies, including assuming duties of a corporate officer. FTC v. Amy Travel Servs., Inc., 875 F.2d 564, 573 (7th Cir. 1989).

An individual defendant is liable for consumer redress if he "had knowledge that the corporation or one of its agents engaged in dishonest or fraudulent conduct, that the misrepresentations were the type which a reasonable and prudent person would rely, and that consumer injury resulted." Publishing Clearing House, 104 F.3d at 1170. In establishing the requisite level of knowledge, the FTC need not establish that the individual possessed the intent to defraud. Amy Travel, 875 F.2d at 573-74. Nor must the FTC establish that the defendant had actual knowledge of the wrongful conduct. Reckless indifference to the wrongful conduct or an awareness of a high probability coupled with an intentional avoidance of the truth will suffice. Id. at 574. (citations and internal quotations omitted).

1. Sam Jain, Daniel Sundin, and Marc D'Souza Are Individually Liable

Defendants Jain, Sundin, and D'Souza each possesses or has possessed the authority to control the IMI Enterprise, and each participated in the conduct at issue. Moreover, each had the requisite level of knowledge to establish individual liability for monetary relief. Jain is the CEO of IMI and Sundin is

the company's COO and CTO. In a small, closely-held corporation like IMI, an individual's status as a corporate officer gives rise to a presumption of such person's ability to control the corporation. See Standard Educ., Inc. v. FTC, 475 F.2d 401, 403 (D.C. Cir. 1973) cert. denied, 414 U.S. 828 (1973). Moreover, in the Canadian lawsuit, both Jain and Sundin acknowledge in sworn affidavits their extensive roles in controlling the activities of the IMI Enterprise. There is also no doubt that Jain and Sundin are fully aware of the deceptive marketing techniques upon which the Defendants rely. According to pleadings filed in the Canadian lawsuit, Marc D'Souza approached Jain with the idea of using the "scanner approach" to market Defendants' software, which Jain approved. See Section III.B(3)(v), *supra*. Also in an affidavit in the Canadian lawsuit, Sundin discussed under oath the aggressive marketing of Defendants' DriveCleaner program and provided a screenshot of one of the bogus scans used to market DriveCleaner. See Section III.B(3)(iii), *supra*.

Although Marc D'Souza appears to have left IMI in late 2006, he is no less culpable. D'Souza was a senior executive with IMI until his departure. D'Souza had extensive control over all of the financial operations of IMI, and was the sole executive responsible for the critically important task of forging relationships with payment processors capable of handling the sales traffic generated by IMI. D'Souza retained tens of millions of dollars of IMI's profits in his bank accounts.[12] See Section III.B(3)(v), *supra*.

---

[12] Injunctive relief as to Marc D'Souza is both necessary and appropriate, despite the fact that he has apparently left IMI. D'Souza holds tens of millions of dollars in liquid assets that are directly traceable to IMI's fraudulent conduct. See Section III.B(3)(v), *supra*. Moreover, D'Souza could easily resume the Defendants' scareware fraud, since he is both the mastermind of the Defendants' fake scan marketing technique and developed the Defendants' critically important relationships with payment processors. Id. See United States v. W. T. Grant Co., 345 U.S. 629, 633 (1945) (an injunction is justified when there is a "cognizable danger of recurrent violation"); SEC v. Lawbaugh, 359 F. Supp. 2d 418, 424-25 (D. Md. 2005) (injunction warranted where this is reasonable likelihood of future violations). The mere discontinuance of an unlawful practice prior to law enforcement action does not deprive a court of the power to grant injunctive relief. U.S. v. Hunter, 459 F.2d 205, 219 (4th Cir. 1971); Nat'l Adver. Co. v. Miami, 402 F.3d 1329, 1333 (11th Cir. 2005).

Moreover, D'Souza's knowledge of the IMI Enterprise's violative conduct is irrefutable. In pleadings filed in the Canadian lawsuit, D'Souza takes credit for developing the scanner-based approach to market IMI's security products and acknowledges that IMI has engaged in "aggressive advertising" that caused the FTC and State Attorneys General to shut down similar operations. Id. D'Souza also acknowledges that the Defendants have gone to great lengths to hide from law enforcement and defrauded consumers. See Section III.D, *supra*.

2. James Reno and Kristy Ross Are Individually Liable

Defendants James Reno and Kristy Ross each possess or has possessed the authority to control the IMI Enterprise, have participated in the conduct at issue, and have the requisite level of knowledge to establish liability for monetary relief. Ross is the Vice President of Business Development for IMI, and has recently assumed some of Defendant Sundin's responsibilities as Chief Operating Officer of the company. See Section III.B(3)(vi), *supra*. Moreover, she is directly responsible for disseminating many of the deceptive ads that have duped consumers into purchasing the Defendants' products, and was made aware on numerous occasions by MyGeek that the ads she was placing were malicious. Id.

James Reno runs the "Ohio office" of the IMI Enterprise, and has played a direct role in the propagation of the Defendants' deceptive advertising. See Section III.B(3)(vii), *supra*. On IMI's behalf, Reno contracted with LimeLight Networks – a content-distribution company that assists entities with high bandwidth needs by duplicating their content on servers around the world – to disseminate deceptive ads and product downloads for a variety of the Defendants' products. Id. As a direct result of Reno's actions, countless consumers were exposed to the Defendants' exploitive advertising.

Reno, too, has the requisite level of knowledge to impose individual liability for monetary relief. Reno was named as a defendant in a private lawsuit brought in 2006, which accused him of being one of the masterminds of the Defendants' scam. Id. Moreover, Reno is the principal of ByteHosting, and runs the Defendants' call center, which routinely delays or denies requests for refunds from defrauded consumers. Id. As a result, Reno cannot credibly deny that he is fully aware of the Defendants'

deceptive practices.

B. The Corporate Defendants Are Liable as a Common Enterprise

As discussed above, the corporate defendants, IMI and ByteHosting, operate as a common enterprise. Courts consider a variety of factors when determining whether a common enterprise exists, including: whether the dealings between the corporations are conducted at an arms length; whether the members of the enterprise operate as a single economic entity; whether business is transacted through a maze of interrelated companies; evidence revealing that no real distinction exists between the corporate defendants; lack of observing corporate formalities; exercise of control over the corporate defendant; product continuity; and work force continuity.[13] When considering whether corporate defendants operate as a common enterprise, "the pattern and frame-work of the whole enterprise must be taken into consideration." Delaware Watch Co. v. FTC, 332 F.2d 745, 746 (2d Cir. 1964).

In this case, a number of facts compel the finding of a common enterprise. The Defendants refer to ByteHosting as the "Ohio office" of IMI, and virtually all of ByteHosting's revenue is received from IMI's accounts. See Section III.B(3)(ii), *supra*. In fact, on numerous occasions, IMI wired funds to ByteHosting for the express purposes of paying payroll, rent, taxes, and utilities. Id.

Moreover, Reno and ByteHosting perform a variety of functions that perpetuate the Defendants' scheme to defraud consumers, including the operation of a "customer support" call center that routinely denies or delays consumers seeking refunds. See Section III.B(3)(ii), *supra*. In addition, James Reno,

---

[13] See CFTC v. Noble Wealth Data Information Svcs, Inc., 90 F. Supp. 2d 676, 691 (D. Md. 2000); Ameridebt, 343 F. Supp. 2d at 451; CFTC v. American Derivatives Corp., Civil Action No. 1:05-CV-2492-RWS, 2008 U.S. Dist. LEXIS 48509 (E.D. Ga. June 23, 2008); CFTC v. Wall Street Underground, Inc., 281 F. Supp. 2d 1260, 1271 (D. Kan. 2003); FTC v. Jordan Ashley, Case No. 93-2257-CIV-NESBITT, 1994 U.S. Dist. LEXIS 7494, *11, 1994-1 Trade Cas. (CCH) P70,570 (S.D. Fla. Apr. 5, 1994); FTC v. Investment Dev., Inc., Civil Action No. 89-642, 1989 U.S. Dist. LEXIS 6502, *29-30 (E.D. La. Jun. 7, 1989); Sunshine Art Studios, Inc. v FTC, 481 F.2d 1171, 1175 (1st Cir. 1973).

ByteHosting's principal, manages critical contracts on IMI's behalf, purchases and maintains computer equipment for IMI. See Section III.B(3)(vii), *supra*. Reno also is connected to at least one of the sham Internet advertising agencies Defendants use to disseminate their deceptive advertising, and has extensive ties to "SetUpAHost," one of the shell companies used by Defendants. Id.

The Defendants operate an unlawful enterprise that does not observe corporate formalities and uses a variety of aliases and shell companies to hide its operations. ByteHosting is an integral part of this unlawful enterprise and should be deemed as part of a common enterprise with IMI, with each corporation liable for the other's acts. See FTC v. Bay Area Bus. Council, Inc., No.: 02 C 5762, 2004 WL 769388, at *12, 2004 U.S. Dist. LEXIS 6192, *33-34 (N.D. Ill. Apr. 8, 2004) (citing FTC v. Think Achievement Corp., 144 F. Supp. 2d 993, 1011 (N.D. Ind. 2000), rev'd in part on other grounds, 312 F.3d 259 (7th Cir. 2002) (participants in a common enterprise held jointly and severally liable for violations of the FTC Act).

C. Relief Defendant Maurice D'Souza Has No Legitimate Claim to Defendants' Ill-Gotten Gains

Maurice D'Souza is named as a relief defendant in this matter because he has received proceeds from the Defendants' fraudulent activities and has no legitimate claim to those funds. Courts may impose equitable relief against those who have: (1) received ill-gotten funds; and (2) do not have a legitimate claim to those funds. CFTC v. Kimberlynn Creek Ranch, Inc., 276 F.3d 187 (4th Cir. 2002) (federal courts may order equitable relief against a person not accused of wrongdoing in a securities enforcement action where that person received ill-gotten funds and did not have a legitimate claim to the funds); see also FTC v. Ameridebt, 343 F. Supp. 2d 451, 464 (D. Md. 2004) (Section 13(b) invests the court with equitable powers over "innocent persons" so as to accomplish such relief as disgorgement of unjust enrichment); SEC v. Antar, 831 F. Supp. 380, 402-03 (D.N.J. 1993) ("As between the nominal defendants and the victims of fraud, equity dictates that the rights of the victims should control.")

Disgorgement of the proceeds of unlawful activity held by a nonparty who has no legitimate

claim to the funds may be ordered under the doctrines of constructive trust or unjust enrichment. See Antar, 831 F. Supp. at 402-03 (court found the nominal defendants liable as constructive trustees and subject to the doctrine of unjust enrichment); Rollins v. Metro. Life Ins. Co., 863 F.2d 1346, 1354 (7th Cir. 1988) ("a constructive trust may be invoked even where the unjustly enriched person is completely blameless."). Under either doctrine, this Court is authorized to disgorge all of the funds Maurice D'Souza received from the Defendants' fraudulent scheme.

Maurice D'Souza, who is Marc D'Souza's father, was directly involved in setting up the various merchant accounts IMI used to process payments for its security products. See Section III.B(3)(viii), *supra*. Maurice D'Souza specifically assisted his son in establishing merchant relationships with various overseas payment processors which allowed IMI to process its credit card transactions for the sale of the Defendants' security products. Id. Although Maurice D'Souza acknowledges that he has no contract or other employment agreement with IMI, at least $18.5 million of IMI's assets reside in his bank accounts. Id. As a result, Maurice D'Souza is a proper relief defendant.

V. AN *EX PARTE* TEMPORARY RESTRAINING ORDER FREEZING ASSETS AND ORDERING THE TURNOVER OF DOCUMENTS, AN ACCOUNTING, AND THE PRESERVATION OF RECORDS SHOULD BE GRANTED

In light of the scope of their fraud, their history of evading law enforcement, and defendant Jain's history of evading service of civil process, Defendants are likely to dissipate assets and destroy records if given notice of the relief sought in this suit. The FTC Act authorizes a district court to use its inherent equitable authority to "grant any ancillary relief necessary to accomplish complete justice." U.S. Oil & Gas, 748 F.2d 1431, 1434 (11th Cir. 1984). The Commission asks that the Court employ that authority here to issue an *ex parte* TRO that freezes the Defendants' assets, requires Defendants to turn over business records to the FTC[14], and orders them to provide the Commission with a financial accounting. Courts in this district and throughout the Fourth Circuit have repeatedly issued TROs *ex*

[14]The FBI executed a search warrant at the business premises of ByteHosting in November 2008. These documents have already been provided to the FTC by the FBI.

parte that contain this type of relief. See cases cited in footnote 8, *supra*.

An *ex parte* TRO is warranted when the facts show that irreparable injury, loss, or damage will result before the defendants can be heard in opposition. See In re Vuitton et Fils, 606 F.2d 1, 4-5 (2d Cir. 1979); Fed. R. Civ. P. 65(b). Here, the Commission seeks, *inter alia*, restitution for the more than one million consumers victimized by Defendants' scheme. The asset freeze requested by the FTC will ensure the possibility of such relief by preventing Defendants from dissipating the proceeds of their fraud before this Court has the opportunity to rule on the merits of this case. Moreover, given the massive scope of the Defendants' unlawful scheme, their extensive use of aliases, shell companies, and false contact information to hide their identities, and their decision to move their operations offshore for the stated purpose of "escap[ing] regulation from the Federal Trade Commission and avoid[ing] State Attorneys who were sanctioning and shutting down similar organizations," it is likely that advance notice of this suit would cause the Defendants to secrete assets and destroy evidence of their unlawful acts. See Section III.D, *supra*.

The FTC's concerns about the destruction of evidence and dissipation of assets absent *ex parte* relief are informed by the Agency's experience with others engaged in similar deceptive schemes. As described in depth in the attached Fed. R. Civ. P. 65(b) declaration, *ex parte* relief has proven essential in preserving assets and preventing the destruction of evidence in similar cases. See Certification and Declaration of Plaintiff's Counsel Ethan Arenson in Support of Plaintiff's *Ex Parte* Motion For: (1) Temporary Restraining Order and Order to Show Cause; and (2) Order Temporarily Sealing Entire File, Ex. 21.

The asset freeze requested by the FTC is well within this Court's authority. An asset freeze should be imposed once the Court determines that the Commission is likely to prevail on the merits and that restitution would be an appropriate remedy at the conclusion of the proceedings. See World Travel, 861 F.2d at 1031 & n.9. (district court at that juncture "had a duty to ensure that" defendants' assets were available for restitution); see also FTC v. Nwaigwe, Civ. No. HAR 96-2690 (D. Md. Aug. 28,

1996) (ordering *ex parte* temporary restraining order with asset freeze); FTC v. Commercial Elec. Supply, Inc., No. WMN 96-1892 (D. Md. June 26, 1996) (ordering *ex parte* temporary restraining order with asset freeze) and other cases cited within footnote 8, *supra*. The freeze here should extend to individual assets as well as corporate assets, because – as demonstrated above – the Commission is likely to succeed in showing that the individual defendants are liable for restitution. See World Travel, 861 F.2d at 1031. The fact that some of these assets are likely outside of the United States is not a bar to the asset freeze requested. See U.S. v. First National City Bank, 379 U.S. 378, 384 (1965) ("Once personal jurisdiction of a party is obtained, the District Court has authority to order it to 'freeze' property under its control, whether the property be within or without the United States."); SEC v. International Swiss Inv. Corp., 895 F.2d 1272, 1276 (9th Cir. 1990) (upholding district court's injunction freezing and ordering an accounting of foreign assets).

Additionally, in order to assist the Commission in locating and securing assets, and to preserve the possibility of consumer redress for victimized consumers and/or the possibility of disgorgement, the FTC requests that the Court order the Defendants to make a full financial accounting.[15] Attached to the proposed Order are copies of proposed financial statements to be completed by each of the Defendants.[16] The Fourth Circuit has upheld the use of these devices, recognizing that they assist the district court's purpose of monitoring compliance with an asset freeze order and in turn ensure effective final relief. See Kemp, 940 F.2d at 113 (affirming district court's order requiring monthly accounting and financial

[15]The TRO also includes a provision that restrains Defendants from taking any action that may result in the encumbrance or dissipation of foreign assets, including taking any action that would invoke a duress clause. This provision is important since Defendants may have created asset protection trusts that could frustrate the Court's ability to provide consumer redress. See FTC v. Affordable Media, 179 F.3d 1228, 1239-44 (9th Cir. 1999).

[16]The TRO also includes a Consent to Release Financial Records form, which allows the FTC to access records of accounts or assets held by foreign financial institutions. This consent form does not abrogate Defendants' fifth amendment or due process rights because it tracks the wording of a consent form found to be non-testimonial in Doe v. United States, 487 U.S. 201, 215 (1988). SEC v. College Bound, 155 F.R.D. 1, 2 (D.D.C. 1994).

disclosure statements); HUD v. Cost Control Mktg. & Sales Mgmt. of Va., 64 F.3d 920, 927 (4th Cir. 1995); Nat'l Org. for Reform of Marijuana Laws v. Mullen, 828 F.2d 536, 544 (9th Cir. 1987) (approving the appointment of a Special Master to monitor compliance with a preliminary injunction).

VI. CONCLUSION

The Defendants are high tech scam artists who have flooded the Internet with false advertising in order to intimidate and frighten consumers into purchasing their security products. In order to put an end to these unlawful practices, we respectfully request that this Court grant the FTC's motion for an *ex parte* TRO and ancillary equitable relief.

Dated: December 2, 2008

Respectfully submitted:

WILLIAM BLUMENTHAL
General Counsel

/s/

Ethan Arenson DC # 473296 (earenson@ftc.gov)
Colleen B. Robbins, NY# 2882710 (crobbins@ftc.gov)
Carmen J. Christopher, DC # 499917 (cchristopher@ftc.gov)
Federal Trade Commission
600 Pennsylvania Ave., NW, Room 288
Washington, D.C. 20580
(202) 326-2204 (Arenson); (202) 326-2548 (Robbins);
(202) 326-3643 (Christopher)
(202) 326-3395 FACSIMILE